Android flaw allows hackers to surreptitiously modify apps

Vulnerability could allow attackers to gain full control of handsets.

by Dan Goodin - July 3 2013, 7:35pm EDT

http://arstechnica.com/security/2013/07/android-flaw-allows-hackers-to-surreptitiously-modify-apps/

Researchers said they've uncovered a security vulnerability that could allow attackers to take full control of smartphones running Google's Android mobile operating system.

The weakness involves the way legitimate Android applications are cryptographically signed to ensure they haven't been modified by parties other than the trusted developer, according to a blog post published Wednesday by researchers from mobile security startup Bluebox. The flaw has existed since at least the release of Android 1.6 almost four years ago. Hackers who exploit the vulnerability can modify app code to include backdoors, keyloggers, or other malicious functionality without changing the verification signature.

Malicious apps that exploit the vulnerability would enjoy the same system privileges as the legitimate one. That access could be especially dangerous if the app that's modified originated with the handset manufacturer or third parties that partner with the manufacturer, Wednesday's blog post said. That's because such apps are typically granted elevated privileges within the Android OS.

"The application then not only has the ability to read arbitrary application data on the device (e-mail, SMS messages, documents, etc.), [and] retrieve all stored account & service passwords, it can essentially take over the normal functioning of the phone and control any function thereof (make arbitrary phone calls, send arbitrary SMS messages, turn on the camera, and record calls)," the blog post said. "Finally, and most unsettling, is the potential for a hacker to take advantage of the always-on, always-connected, and always-moving (therefore hard-to-detect) nature of these “zombie” mobile devices to create a botnet."

While it would be devastating if an attacker was able to get such a modified APK into the Google Play Store, or somehow use the technique to hijack the update mechanism of legitimate apps, there are probably safeguards already in place to prevent such attacks.

"I imagine that Google would move quickly to add some logic to look for such attacks," Dan Wallach, a professor specializing in Android security in the computer science department of Rice University, told Ars. "Without that available to an attacker, this is likely to only be relevant for Android users who use third-party app stores (which have lots of other problems). This bug could also be valuable for users trying to 'root' their phones."

Blue box researchers privately reported the vulnerability to Google in February.